UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,235	11/30/2005	Majid Shahbazi	40732-215150	9977

22204   7590   12/12/2006

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER
NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/527,235	SHAHBAZI, MAJID
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>28 September 2006</u>.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>17-21,26,27 and 33-40</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>17-21,26,27 and 33-40</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in response to applicants' response filed on 9/28/06.

2.   Claims 17-21, 26, 27 and 33-40 are pending.

3.   Applicant's arguments have been fully considered but they are not persuasive.

4.   When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

Response to Arguments

1.   Applicant on page 6, lines 15-17 of the remarks argues that "There is no suggestion whatsoever in Albert to use a computing node located on the network side of the network connection between the computing node and one or more mobile devices."

The examiner respectfully disagrees and asserts that Albert discloses a network that connects a plurality of clients via a gateway to server corresponding to the recited computing node (see, for example, Figs. 3 & 4 and [0071]).

2.   Applicant on page 6, lines 18-20 of the remarks argues that "to verify, from the network side of the network connection, that the right security policies are enforced on the mobile device, as is recited in claim 17."

Claim 17 does not recite the above limitation.

3.   Applicant on page 6, lines 20-23 of the remarks argues that "Albert fails to disclose managing, from the network side of the network connection, at least one security process between the computing node and one or more mobile devices based on the at least one security parameter determined by interpreting the node security profile, as is recited in claim 17."

The examiner respectfully disagrees and asserts that Albert discloses that upon the request by a client to connect to the network server, the server performs an evaluation process to determine the version of the security policy installed on the client (e.g. pg. 8, [0072], lines 8-27). If the client does not have the most current version of the security policy, the server will download it onto the client. This operation performed by the server corresponds (i.e., equivalent) to the recited limitation stated above.

4.   Applicant on page 6, lines 20-23 of the remarks argues that "Sharma fails to disclose or suggest running a discovery program to detect one or more mobile devices or resources."

The examiner respectfully disagrees and asserts that Sharma discloses a server that capable of finding the location of a particular asset (corresponding to the recited mobile device or resource) (e.g. [0008]). Sharma further discloses a network management server that includes a module called network discovery process (e.g. Fig. 4, block 426) that is capable of discovering the network physical assets and links (corresponding to the recited detect one or more mobile devices or resources) (e.g. [0071]).

5.   The examiner, however, in light of the above submission maintains the previous

rejections while considering the amendments to the claims 1 and 33 as follows:

Claim Objections

Claim 39 is objected to because of the following informalities: The term

"analyses" should be replaced with term "analyzed". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 17-21 and 26-27 are rejected under 35 U.S.C. 102(e) as being

anticipated by Albert et al (2003/0177389 A1; hereinafter Albert).

Regarding claim 17, Albert discloses:

A method for securing a computer system that includes one or more mobile

devices located on a user's side of a network connection and a computing node located

on a network side of the network connection, (see, for example, Figs. 3 & 4; [0008]),

comprising:

executing a node security program in the computing node for interpreting a node

security profile (see, for example, [0024]-[0025]; [0121]);

determining at least one security parameter from the interpretation of the node

security profile (see, for example, [0047]-[0049]; [0118]); and

managing, from the network side of the network connection, at least one security

process between the computing node and one or more mobile devices based on the at

least one security parameter determined by interpreting the node security profile (see,

for example, [00011]; [00014]; [0024]; Figs. 3 & 4; [0071]), and

transferring a device security profile to a mobile device or a resource device to be

interpreted by a device security program running on the mobile device to determine

device security parameters (see, for example, [0042]; [0066]; [0072]; [0084]).

Regarding claim 18, Albert discloses:

The method of claim 17, wherein transferring the device security profile

comprises accessing at least one of a server station, a central station, and a computing

node or a website (see, for example, [0008]; [0044]).

Regarding claim 19, Albert discloses:

The method of claim 17, wherein the device security profile is transferred based

on at least one of a temporal attribute and a position of the mobile device in at least one

of real time or non-real time modes (see, for example, [0011]; [0014]; [0121).

Regarding claim 20, Albert discloses:

The method of claim 17 further comprising periodically updating at least one of the node security profile and device security profile (see, for example, [0014]; [0062]; [0066).

Regarding claim 21, Albert discloses:

The method of claim 17, wherein the step of transferring includes at least one of a data synchronization process, data transfer, file transfer, and an email between the computing node and a mobile device ore resource (see, for example, [0072]; [0085]; [0110]).

Regarding claim 26, Albert discloses:

The method of claim 17 further including transmitting at least one of the node security profile and device security profile using at least one of a push or pull technology (see, for example, [0062]; [0066]).

Regarding claim 27, Albert discloses:

The method of claim 17 further including transmitting at least one of the node security profile and device security profile using an over the air protocol (see, for example, [0008]; [0049]; [0065]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 33-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al (2003/0177389 A1; hereinafter Albert) as applied to claim 17 above, and further in view of Sharma et al (2002/0068559 A1; hereinafter Sharma).

Regarding claim 33, Albert discloses:

using the determined mobile device information for managing security of the computer system (see, for example, [00011]; [00014]; [0024]).

Albert, however, does not expressly disclose:

A method for managing a computer system including a computing node and one or more mobile devices, comprising:

running a discovery program to detect one or more mobile devices or resources;

determining information regarding one or more mobile devices or resources based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an executable program and attributes associated with a mobile device or resource.

using the determined mobile device information for managing to manage security of the computer system from the network side of the network connection (see, for example, Figs. 3 & 4; [0071]).

Sharma discloses:

A method for managing a computer system including a computing node and one or more mobile devices (see, for example, abstract; [0010]-[0012]), comprising:

running a discovery program to detect one or more mobile devices or resources (see, for example, [0061]-[0062]; [0066]-[0067]);

determining information regarding one or more mobile devices or resources based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an·executable program and attributes associated with a mobile device or resource (see, for example, [0020]; [0039]; [0047]; [0064]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement in the system of Albert, a computer system management program for the discovery and detection of mobile devices in the system as taught in Sharma, because it would provide a mechanism to manage network assets via a secure communication path (Sharma, [0010]).

Regarding claim 34, Sharma discloses:

The method of claim 33 further including scanning the computer system based on a scan profile to detect the one or more mobile devices (see, for example, [0021], where the configuration data corresponds to the recited profile; [0027]; [0113]).

Regarding claim 35, Sharma discloses:

The method of claim 33, wherein the discovery program is run in at least one of a

remote central station or a local computing node (see, for example, [0010]; [0091]).

Regarding claim 36, Sharma discloses:

The method of claim 33 further including grouping the located mobile devices or

resources by type and other attribute (see, for example, [0059]; [0062]).

Regarding claim 37, Sharma discloses:

The method of claim 34, wherein the scan profile contains information regarding

at least one of network, domain, IP address, netmask, and computer identity to be

scanned, time of synchronization and device connection (see, for example, [0076]).

Regarding claim 38, Sharma discloses:

The method of claim 34, wherein the scan profile contains information regarding

at least one of network, domain, IP address, netmask, and computer identity not to be

scanned (see, for example, [0076]; [0090]; [0140]-[0141]).

Regarding claim 39, Sharma discloses:

The method of claim 34, wherein the results of scanning are analyses and

populated and stored and displayed to the users (see, for example, [0022]; [0034];

[0059]).

Note: Examiner assumed "analyzed" instead of the word "analyses" above due to a typo (see specification, page 6, lines 20-21).

Regarding claim 40, Sharma discloses:

The method of claim 33, wherein the gather mobile device information include at least one of device type, device identity, synchronization software type, synchronization software availability, synchronization software location, synchronization software version number, previous synchronization information, data and time of last synchronization, the type of device used during previous synchronization, synchronization ID, device owner information, type of applications and files installed or used on the mobile device, file size, file name, file attribute, manufacturer information, time of all completed and incomplete synchronization and data access and connections performed, type of data and information transferred to and from a mobile device and a resource (see, for example, [0022]; [0030]; [0038]; [0059]; [0090]).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

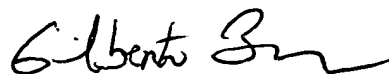than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-

272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 10, 2006   Abdulhakim Nobahar
                                                             Examiner, Art Unit 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100